(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 552 392 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **92101016.1**

(51) Int. Cl.5: **G07F 7/10**, H04L 9/32

(22) Anmeldetag: **22.01.92**

(43) Veröffentlichungstag der Anmeldung:
28.07.93 Patentblatt 93/30

(84) Benannte Vertragsstaaten:
AT BE CH DE ES FR GB IT LI NL SE

(71) Anmelder: **Siemens Nixdorf Informationssysteme Aktiengesellschaft**
Fürstenallee 7
W-4790 Paderborn(DE)

(72) Erfinder: **Hewel, Harald, Dipl.-Ing.**
Lilienstrasse 22
W-8890 Aichach(DE)

Erfinder: **Gefrörer, Stanislaus, Dipl.-Math.**
Flurweg 34
W-8028 Taufkirchen(DE)

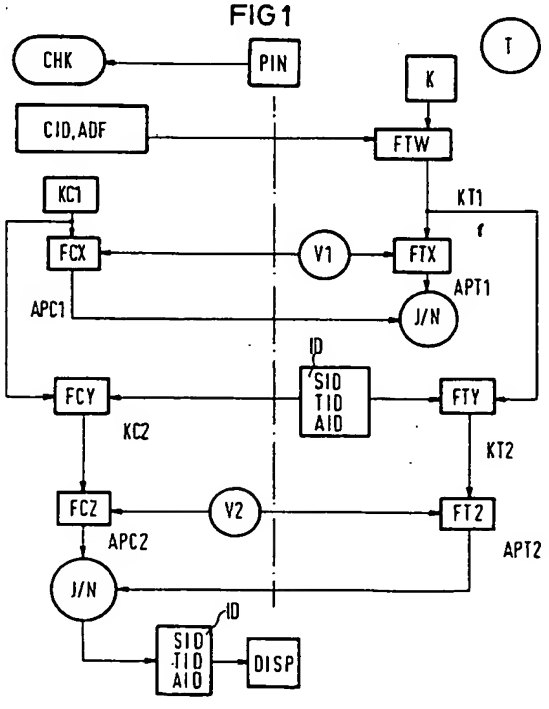
Erfinder: **Kruse, Dietrich Dipl.-Ing.**
Ulmenstrasse 9
W-8012 Ottobrunn(DE)

(74) Vertreter: **Fuchs, Franz-Josef, Dr.-Ing. et al**
Postfach 22 13 17
W-8000 München 22 (DE)

(54) Verfahren zur gegenseitigen Authentifikation einer Chipkarte und eines Terminals.

(57) Das angegebene Verfahren ergänzt die Challenge- and Response-Methode zur gegenseitigen Authentifikation einer Chipkarte (CHK) und eines Terminals (T). Mit Hilfe von Identitätskenngrößen (ID) für das Terminal (T), die laufende Anwendung und das im Terminal (T) befindliche Sicherheitsmodul, einer Verschlüsselungsfunktion (FCY,FTY) und des chipkartenspezifischen Schlüssels (KC1,KT1) wird vor Authentitätsprüfung des Terminals (T) ein terminalspezifischer Schlüssel (KC2,KT2) berechnet. Die Identitätskenngrößen (ID) werden nach erfolreichem Abschluß der Authentizitätsprüfung optisch und/oder akustisch dem Chipkartenbenutzer mitgeteilt.

FIG 1



EP 0 552 392 A1

Die Erfindung betrifft ein Verfahren zur gegenseitigen Authentifikation einer Chipkarte und eines Terminals nach der Challenge- and Response-Methode. Üblicherweise authentifiziert sich zunächst die Chipkarte gegenüber dem Terminal. Die Chipkarte überträgt ihre Chipkartenidentitätsnummer zum Terminal. Dieses berechnet aus der Chipkartenidentitätsnummer einen ersten Terminalschlüssel, der bei Verwendung symmetrischer Verschlüsselungsalgorithmen mit einem ersten in der Chipkarte gespeicherten Chipkartenschlüssel identisch ist. Nun generiert das Terminal eine erste Zufallszahl, überträgt sie zur Chipkarte und das Terminal verschlüsselt die erste Zufallszahl ebenso wie die Chipkarte. Als Verschlüsselungsergebnis liegt sowohl in der Chipkarte als auch im Terminal ein erster Anerkennungsparameter vor. Diese beiden Anerkennungsparameter werden im Terminal verglichen. Bei positivem Vergleichsergebnis ist die Chipkarte authentisch.

Zur Authentifikation des Terminals gegenüber der Chipkarte findet der oben beschriebene Vorgang mit vertauschten Rollen statt. Der bereits beiden Partnern bekannte erste Schlüssel wird zur beiderseitigen Verschlüsselung einer von der Chipkarte generierten Zufallszahl verwendet. Die dabei entstehenden zweiten Anerkennungsparameter werden in der Chipkarte verglichen. Bei positivem Vergleichsergebnis ist auch das Terminal authentisch.

Die Chipkarte erhält damit zwar Gewißheit darüber, ob das Terminal, mit dem sie verbunden ist, authentisch ist. Die Chipkarte erhält aber keine Kenntnis darüber, um welches von vielen möglichen Terminals es sich handelt. Dieses Informationsdefizit könnte zwar zum Beispiel durch das Übertragen einer Terminalnummer zur Chipkarte beseitigt werden, jedoch kann eine solche Informationsübertragung zu Sicherheitdefiziten, z.B. durch Offenbarung der Identitätskenngröße an Dritte, führen. Der Benutzer der Chipkarte kann sich von der Authentizität des Terminals nicht selbst überzeugen, denn der Benutzer erhält entweder keine oder nur eine subjektive Information darüber, daß die Authentizitätsprüfung erfolgreich verlaufen ist.

Die der vorliegenden Erfindung zugrundeliegende Aufgabe ist es, eine sichere Identifikation aller sicherheitsrelevanten Elemente eines Terminals gegenüber einer Chipkarte zu ermöglichen und darüberhinaus dem Benutzer der Chipkarte die Möglichkeit zu geben, sich objektiv von der Authentizität des Terminals zu überzeugen.

Diese Aufgabe wird erfindungsgemäß durch die im Patentanspruch 1 angegebenen Merkmale gelöst.

Gemäß dem im Patentansprucr 1 angegebenen Verfahren wird die bzw. werden die Identitätskenngrößen, die dem Terminal T zugeordnet sind, in den gegenseitigen Authentifikationsprozeß gemäß der Challenge- and Response-Methode mit einbezogen. Es wird nicht nur ein chipkartenspezifischer Schlüssel verwendet, sondern dieser chipkartenspezifische Schlüssel wird zur Generierung eines zweiten terminal- und chipkartenspezifischen Schlüssels verwendet. Damit ist eine eindeutige und sichere Identifikation inklusive einer Authentifikation aller Elemente des Terminals gewährleistet, deren Kenngrößen Bestandteil der zur Chipkarte übertragenen Identitätskenngröße sind.

Bei Übereinstimmen der ersten und der zweiten Anerkennungsparameter werden die dem Terminal zugeordneten Identitätskenngrößen und/oder eine diese Identitätskenngrößen repräsentierende Information optisch und/oder akustisch angezeigt. Diese Anzeige erfolgt auf einer Anzeigeeinheit. Diese Anzeigeeinheit kann ein Lautsprecher, eine Flüssigkristallanzeige oder ähnliches sein.

Durch eine solche Anzeige kann sich der Chipkartenbenutzer selbst davon überzeugen, daß das Terminal weder manipuliert noch simuliert ist. Erleichtert wird dies dem Benutzer dann, wenn die die Identitätskenngrößen repräsentierende Information ein Wort ist, das eindeutig der oder den Identitätskenngrößen zugeordnet ist. Die Vertrauenswürdigkeit des Terminals wird durch die Anzeige für den Chipkartenbenutzer nachgewiesen.

Gemäß einer weiteren Weiterbildung der Erfindung muß das angezeigte Ergebnis quittiert werden. Diese Quittierung erfolgt beispielsweise durch einen Tastendruck oder durch Ablauf einer hinreichend langen Zeit.

Gemäß einer Ausgestaltung und Weiterbildung der Erfindung ist im Terminal ein Sicherheitsmodul integriert, dessen Sicherheitsidentitätskenngrößegemeinsam mit einer Terminalidentitätskenngröße zur Chipkarte übertragen wird. Diese beiden Identitätskenngrößen bilden die dem Terminal zugeordnete Identitätskenngröße. Die Chipkarte erhält damit auch eine gesicherte und authentische Information darüber, welches Sicherheitsmodul aktuell im Terminal integriert ist.

Gemäß einer weiteren Weiterbildung der Erfindung wird gemeinsam mit der dem Terminal zugeordneten Identitätskenngröße eine Anwendungsidentitätksenngröße zur Chipkarte übertragen. Die Identitätskenngröße wird also um eine Anwendungsidentitätskenngröße erweitert. Damit ist es der Chipkarte auch möglich, die im Terminal laufende Anwendung im Zusammenhang mit der Chipkarte eindeutig zu identifizieren und deren Authentizität zu überprüfen.

Gemäß einer weiteren Weiterbildung und Ausgestaltung der Erfindung wird vom Zeitpunkt der Übertragung bzw. der Eingabe einer Personenkennzahl aus bzw. in das Terminal jegliche Anzeige auf Seiten des Terminals verhindert. Diese Verhin-

derung jeglicher Anzeige wird erst nach Anzeige der Identitätskenngrößen und/oder der diese Identitätskenngrößen repräsentierenden Information wieder aufgehoben. Damit kann also von Seiten des Terminals bis zur Feststellung der Authentizität durch die Chipkarte die Anzeigeeinheit des Terminals nicht aktiviert werden. Eine Anzeige manipulierter Informationen ist somit wirksam verhindert.

Gemäß einer weiteren Ausgestaltung und Weiterbildung der Erfindung werden die zwischen Chipkarte und Terminal auszutauschenden Daten über ein zwischen Chipkarte und Terminal angeordnetes Chipkartenterminal geleitet. Die dem Terminal zugeordneten Identitätskenngrößen und/oder eine diese Identitätskenngrößen repräsentierende Information wird mit Hilfe der auf dem Chipkartenterminal angeordneten Anzeigeeinheit angezeigt. Diese Anzeige wird durch eine benutzerseitige Betätigung der auf dem Chipkartenterminal angeordneten Tastatur quittiert. Durch diese Ausgestaltung und Weiterbildung der Erfindung wird auf Grund der räumlichen Trennung von Chipkartenterminal und Terminal ein zusätzlicher Schutz vor einer Manipulation der Anzeigeeinheit des Terminals erreicht. Das Chipkartenterminal kann zusätzlich von der Chipkarte aufgefordert werden sich unabhängig vom Terminal selbst gegenüber der Chipkarte zu authentisieren. Durch diese zusätzliche Möglichkeit wird deutlich, daß das Chipkartenterminal sicherheitstechnisch gesehen der Chipkarte zugeordnet ist. Das Chipkartenterminal wirkt dabei vor allem als vertrauenswürdige Schnittstelle zwischen Chipkarte und Chipkartenbenutzer. Die gleiche Vertrauenswürdigkeit ist bei einer Integration der Funktionen des Chipkartenterminals im Terminal nur mit großem Aufwand erreichbar.

Gemäß einer weiteren Weiterbildung und Ausgestaltung der Erfindung wird vor jeder gegenseitigen Authentifikation der Chipkarte und des Terminals eine Überprüfung der eingegebenen Personenkennzahl durchgeführt. Damit ist gewährleistet, daß eine Anzeige an der Anzeigeeinheit während des Verfahrens zur gegenseitigen Authentifikation von Chipkarte und Terminal stets verhindert ist, auch wenn die Chipkarte für mehrere verschiedene Anwendungen geeignet ist. Daraus folgt zwar, daß eine globale Prüfung der Personenkennzahl für mehrere Anwendungen nicht möglich ist. Dieser Nachteil wird aber durch den Gewinn an Sicherheit mehr als aufgewogen.

Weitere vorteilhafte Ausgestaltungen und Weiterbildungen sind in weiteren Unteransprüchen angegeben. Im folgenden wir die Erfindung anhand der Zeichnung näher erläutert. Dabei zeigen:

FIG 1 das erfindungsgemäße Ablaufdiagramm gemäß der Challenge- and Response-Methode,

FIG 2 eine schematisch dargestellte Anordnung einer Chipkarte, eines Chipkartenterminals und eines Zentralrechners, und

FIG 3 eine Anordnung gemäß FIG 2, bei der das Chipkartenterminal mit einer Rechnerstation in einem Terminal integriert ist.

Im folgenden Ausführungsbeispiel wird das erfindungsgemäße Verfahren, wie es in Figur 1 dargestellt ist, beschrieben. Als Kommunikationspartner werden dabei ein Terminal T und eine Chipkarte CHK verwendet. Das Terminal T umfaßt dabei sämtliche Einheiten außerhalb der Chipkarte CHK. Solche Einheiten sind beispielsweise ein Chipkartenterminal CKT, ein Zentralrechner HOST, eine Rechnerstation CPU, und Leitungssysteme L.

Das Chipkartenterminal CKT bildet die Schnittstelle sowohl zwischen Chipkarte CHK und Zentralrechner HOST als auch zwischen Chipkarte CHK und Chipkartenbenutzer. Im Chipkartenterminal CKT sind eine Anzeigeeinheit DISP und ein Eingabetastenblock TAS integriert.

In Figur 2 ist das Chipkartenterminal CKT eine Einzeleinheit, die über das Leitungssystem L mit dem Zentralrechner HOST verbunden ist. In Figur 3 kann das Chipkartenterminal CKT sowohl eine Einzeleinheit, als auch eine Einheit sein, die gemeinsam mit der Rechnerstation CPU im Terminal T integriert ist.

In welcher räumlichen Form das Chipkartenterminal CKT auch immer vorliegt - wichtig für das erfindungsgemäße Verfahren ist die absolute Vertrauenswürdigkeit der im Chipkartenterminal CKT implementierten Einheiten, nämlich der Anzeigeeinheit DISP DISP und der Tastatur TAS.

Das Ausführungsbeispiel beschreibt die Challenge and Response-Methode bei Verwendung von symmetrischen Verschlüsselungsalgorithmen. Das erfindungsgemäße Verfahren ist jedoch ebenso mit asymmetrischen Verschlüsselungsalgorithmen durchführbar. Dazu müssen lediglich die verwendeten Funktionen und die verwendeten Schlüssel entsprechend den Anforderungen des asymmetrischen Verschlüsselungsverfahrens angepaßt werden.

In Figur 1 sind links von einer strichpunktierten Linie die Verfahrensabläufe eingetragen, die in der Chipkarte CHK ablaufen, rechts der strichpunktierten Linie sind die Verfahrensabläufe dargestellt, die im Terminal T, und dort insbesondere in einem Sicherheitsmodul ablaufen. Nach Verbinden der Chipkarte CHK mit dem Terminal T gibt ein Chipkartenbenutzer mit Hilfe des terminalseitigen Tastenfeldes TAS eine Personenkennzahl PIN ein. Nach dieser Eingabe wird jede Anzeige auf der Anzeigeeinheit DISP des Terminals T verhindert. Die Personenkennzahl PIN wird zu Vergleichszwekken zur Chipkarte CHK übertragen. Bei positivem

Vergleichsergebnis überträgt die Chipkarte CHK ihre Chipkartenidentitätsnummer CID und ein die gewünschte Anwendung kennzeichnendes Applikationskommando ADF zum Terminal T. Im Terminal T wird mit Hilfe der empfangenen Daten, einem im Terminal T gespeicherten Schlüssel K und eines Algorithmus FTW ein erster Terminalschlüssel KT1 errechnet. Dieser erste Terminalschlüssel KT1 entspricht dem in der Chipkarte CHK gespeicherten ersten Chipkartenschlüssel KC1.

Im Terminal T wird eine erste Zufallszahl V1 generiert und zur Chipkarte CHK übertragen. Sowohl in der Chipkarte CHK als auch im Terminal T werden nun erste Anerkennungsparameter APC1, APT1 errechnet. Auf Seiten der Chipkarte CHK geschieht dies mit Hilfe der ersten Zufallszahl V1, des ersten Chipkartenschlüssels KC1 und einer ersten Chipkartenfunktion FCX. Die erste Chipkartenfunktion FCX entspricht einer ersten Terminalfunktion FTX.

Das Terminal T errechnet einen ersten Terminalanerkennungsparameter APT1 mit Hilfe der ersten Zufallszahl V1, des ersten Terminalschlüssels KT1 und der ersten Terminalfunktion FTX. Der von der Chipkarte CHK errechnete erste Chipkartenanerkennungsparameter APC1 wird zum Terminal T übertragen und dort mit dem ersten Terminalanerkennungsparameter APT1 verglichen. Bei negativem Vergleichsergebnis wird das Verfahren abgebrochen, da dann die Chipkarte CHK nicht authentisch ist.

Bevor nun auch die Authentizität des Terminals T gegenüber der Chipkarte CHK überprüft wird, errechnet die Chipkarte CHK einen zweiten Chipkartenschlüssel KC2 und das Terminal T einen zweiten Terminalschlüssel KT2. In der Chipkarte CHK erfolgt dies nach Übertragen von dem Terminal T zugeordneten Identitätskenngrößen ID an die Chipkarte CHK. Die Chipkarte CHK bildet aus den Identitätskenngrößen ID und dem ersten Chipkartenschlüssel KC1 mit Hilfe einer zweiten Chipkartenfunktion FCY den zweiten Chipkartenschlüssel KC2. Das Terminal T bestimmt aus den Identitätskenngrößen ID, dem ersten Terminalschlüssel KT1 und einer zweiten Terminalfunktion FTY den zweiten Terminalschlüssel KT2. Die zweite Chipkartenfunktion FCY und die zweite Terminalfunktion FTY sind identisch.

Die dem Terminal T zugeordneten Identitätskenngrößen ID sind eine Sicherheitsidentitätskenngröße SID, eine Terminalidentitätskenngröße TID und eine Anwendungsidentitätskenngröße AID. Die Sicherheitsidentitätskenngröße SID bezeichnet eindeutig ein bestimmtes Sicherheitsmodul. Die Terminnalidentitätskenngröße TID bezeichnet eindeutig ein bestimmtes Terminal T. Ebenso bezeichnet die Anwendungsidentitätskenngröße AID eindeutig eine bestimmte aktuell ablaufende Anwendung. Die zweiten Schlüssel KC2, KT2 in der Chipkarte CHK und im Terminal T verändern sich demzufolge, wenn die Anwendung geändert wird, wenn ein anderes Sicherheitsmodul ins Terminal T integriert wird, oder wenn eine Verbindung mit einem anderen Terminal T erfolgt.

Bevor die Identitätskenngröße ID vom Terminal T zur Chipkarte CHK übertragen wird, kann diese Identitätskenngröße ID mit Hilfe eines "Message Authentification Code" zusätzlich gesichert werden.

Zur Authentifikation des Terminals T gegenüber der Chipkarte CHK erzeugt nun die Chipkarte CHK eine zweite Zufallszahl V2 und überträgt diese zum Terminal T. Das Terminal T berechnet mit Hilfe einer dritten Terminalfunktion FTZ, des zweiten Terminalschlüssels KT2 und der zweiten Zufallszahl V2 einen zweiten Terminalanerkennungsparameter APT2 und überträgt diesen zur Chipkarte CHK. Die Chipkarte errechnet aus dem zweiten Chipkartenschlüssel KC2, der zweiten Zufallszahl V2 und einer dritten Chipkartenfunktion FCZ einen zweiten Chipkartenanerkennungsparameter APC2. Die zweiten Anerkennungsparameter AP2 werden in der Chipkarte CHK verglichen. Bei positivem Vergleichsergebnis werden die Identitätskenngrößen ID von der Chipkarte CHK zum Terminal T übertragen und mit Hilfe der Anzeigeeinheit DISP des Terminals T angezeigt. Diese Anzeige erfolgt in Form einer die Identitätskenngrößen ID repräsentierenden Information. Dieser Information - z.B. ein bestimmtes Wort - ist eindeutig das Tripel bestehend aus Sicherheitsidentitätskenngröße SID, Terminalidentitätskenngröße TID und Anwendungsidentitätskenngröße AID zugeordnet. Erkennt der Chipkartenbenutzer dieses Wort als richtig an, dann ist für ihn das Terminal T objektiv authentisch.

Die Bekanntgabe des Ergebnisses der Authentizitätsprüfung kann jedoch auch unmittelbar durch die Chipkarte CHK erfolgen. Voraussetzung dafür ist, daß die Chipkarte über eine Anzeigeeinheit DISP, wie z.B. Leuchtdioden, einen akustischen Signalgeber, der beispielsweise bestimmte Tonfolgen abzugeben vermag oder eine Flüssigkristallanzeige verfügt.

Mit der Anzeige der die Identitätskenngrößen ID repräsentierenden Information wird die Anzeigeeinheit DISP wieder für die Anzeige anderer Informationen freigegeben. Ist eine Quittierung der angezeigten Identitätskenngrößen ID durch den Chipkartenbenutzer vorgesehen, dann erfolgt die Freigabe der Anzeigeeinheit DISP erst nach dieser Quittierung.

Patentansprüche

1. Verfahren zur gegenseitigen Authentifikation einer Chipkarte und eines Terminals mittels fol-

gender Schritte:

- die Chipkarte überträgt zumindest eine Chipkartenidentifikationsnummer (CID) zum Terminal (T)
- das Terminal (T) bestimmt aus der Chipkartenidentifikationsnummer (CID) einen ersten Terminalschlüssel (KT1)
- die Chipkarte (CHK) bzw. das Terminal (T) berechnet aus einem ersten Chipkartenschlüssel (KC1) bzw. dem ersten Terminalschlüssel (KT1) und einer ersten Zufallszahl (V1) mit Hilfe einer ersten Chipkartenfunktion (FCX) bzw. einer ersten Terminalfunktion (FTX) einen ersten Chipkartenanerkennungsparameter (APC1) bzw. einen ersten Terminalanerkennungsparameter (APT1)
- die Chipkarte (CHK) überträgt den ersten Chipkartenanerkennungsparameter (APC1) zum Terminal (T), wo die beiden ersten Anerkennungsparameter (APC1,APT1) miteinander verglichen werden
- das Terminal (T) überträgt bei positivem Vergleichsergebnis mindestens eine dem Terminal (T) zugeordnete Identitätskenngröße (ID) zur Chipkarte (CHK)
- die Chipkarte (CHK) bzw. das Terminal (T) berechnet aus dem ersten Chipkartenschlüssel (KC1) bzw. aus dem ersten Terminalschlüssel (KT1) und der Identitätskenngröße (ID) mit Hilfe einer zweiten Chipkartenfunktion (FCY) bzw. einer zweiten Terminalfunktion (FTY) einen zweiten Chipkartenschlüssel (KC2) bzw. einen zweiten Terminalschlüssel (KT2)
- die Chipkarte (CHK) bzw. das Terminal (T) berechnet aus dem zweiten Chipkartenschlüssel (KC2) bzw. aus dem zweiten Terminalschlüssel (KT2) und einer zweiten Zufallszahl (V2) mit Hilfe einer dritten Chipkartenfunktion (FCZ) bzw. einer dritten Terminalfunktion (FTZ) einen zweiten Chipkartenanerkennungsparameter (APC2) bzw. einen zweiten Terminalanerkennungsparameter (APT2)
- das Terminal (T) überträgt den zweiten Terminalanerkennungsparameter (APT2) zur Chipkarte (CHK), wo die beiden zweiten Anerkennungsparameter (APC2,APT2) miteinander verglichen werden und
- bei Übereinstimmen der ersten und der zweiten Anerkennungsparameter (APC1, APT1, APC2, APT2) werden die dem Terminal (T) zugeordneten Identitätskenngrößen (ID) und/oder eine diese Identitätskenngrößen (ID) repräsentierende Information optisch und/oder akustisch mit Hilfe einer Anzeigeeinheit (DISP) angezeigt.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß im Terminal (T) der erste Terminalschlüssel (KT1) mit Hilfe eines Algorithmus (FTW) aus der Chipkartenidentifikationsnummer (CID) und einem Schlüssel (K) berechnet wird.

3. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Anzeige der Identitätskenngrößen (ID) und/oder der diese Identitätskenngrößen (ID) repräsentierenden Information auf Seiten des Terminals (T), insbesondere auf der Anzeigeeinheit (DISP) eines Chipkartenterminals (CKT), erfolgt.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Richtigkeit der angezeigten Identitätskenngrößen (ID) und/oder der die Identitätskenngrößen (ID) repräsentierenden Information quittierbar ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem vor einer Übertragung der Chipkartenidentifikationsnummer (CID) zum Terminal (T) vom Terminal (T) eine von einem Chipkartenbenutzer in das Terminal (T), insbesondere in eine Tastatur (TAS) eines Chipkartenterminals (CKT), eingegebene Personenkennzahl (PIN) zu einem Vergleich zur Chipkarte (CHK) übertragen wird, **dadurch gekennzeichnet,** daß mit der Übertragung bzw. der Eingabe der Personenkennzahl (PIN) jegliche Anzeige der Anzeigeeinheit (DISP) auf Seiten des Terminals (T) , insbesondere des Chipkartenterminals (CKT), verhindert wird und daß nach Anzeige der Idenitiätskenngrößen (ID) und/oder der diese Identitätskenngrößen (ID) repräsentierenden Information die Verhinderung der Anzeige auf Seiten des Terminals (T) aufgehoben wird.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet,** daß erst nach Quittieren der Richtigkeit der angezeigten Identitätskenngrößen (ID) und/oder der die Identitätskenngrößen (ID) repräsentierenden Information die Verhinderung der Anzeige auf Seiten des Terminals (T), insbesondere des Chipkartenterminals (CKT), aufgehoben wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß im Terminal (T) ein Sicherheitsmodul integriert ist, dessen Sicherheitsidentitätskenngröße (SID) gemeinsam mit einer Terminalidentitätskenngröße (TID) zur Chipkarte übertragen wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß gemeinsam mit der Sicherheitsidentitätskenngröße (SID) und der Terminalidentitätskenngröße (TID) eine Anwendungsidentitätskenngröße (AID) zur Chipkarte (CHK) übertragen wird.

9. Verfahren nach einem der Ansprüche 4 bis 8, **dadurch gekennzeichnet,** daß die zwischen Chipkarte (CHK) und Terminal (T) auszutauschenden Daten über ein zwischen Chipkarte (CHK) und Terminal (T) angeordnetes Chipkartenterminal (CKT) geleitet werden, daß die dem Terminal (T) zugeordneten Identitätskenngrößen (ID) und/oder eine diese Identitätskenngrößen (ID) repräsentierende Information mit Hilfe der auf dem Chipkartenterminal (CKT) angeordneten Anzeigeeinheit (DISP) angezeigt werden und daß die Anzeige durch eine benutzerseitige Betätigung einer auf dem Chipkartenterminal (CKT) angeordneten Tastatur (TAS) quittiert wird.

10. Verfahren nach einem der Ansprüche 5 bis 9, **dadurch gekennzeichnet,** daß vor jeder gegenseitigen Authentifikation der Chipkarte (CHK) und des Terminals (T) eine Überprüfung der eingegebenen Personenkennzahl (PIN) erfolgt.

FIG1

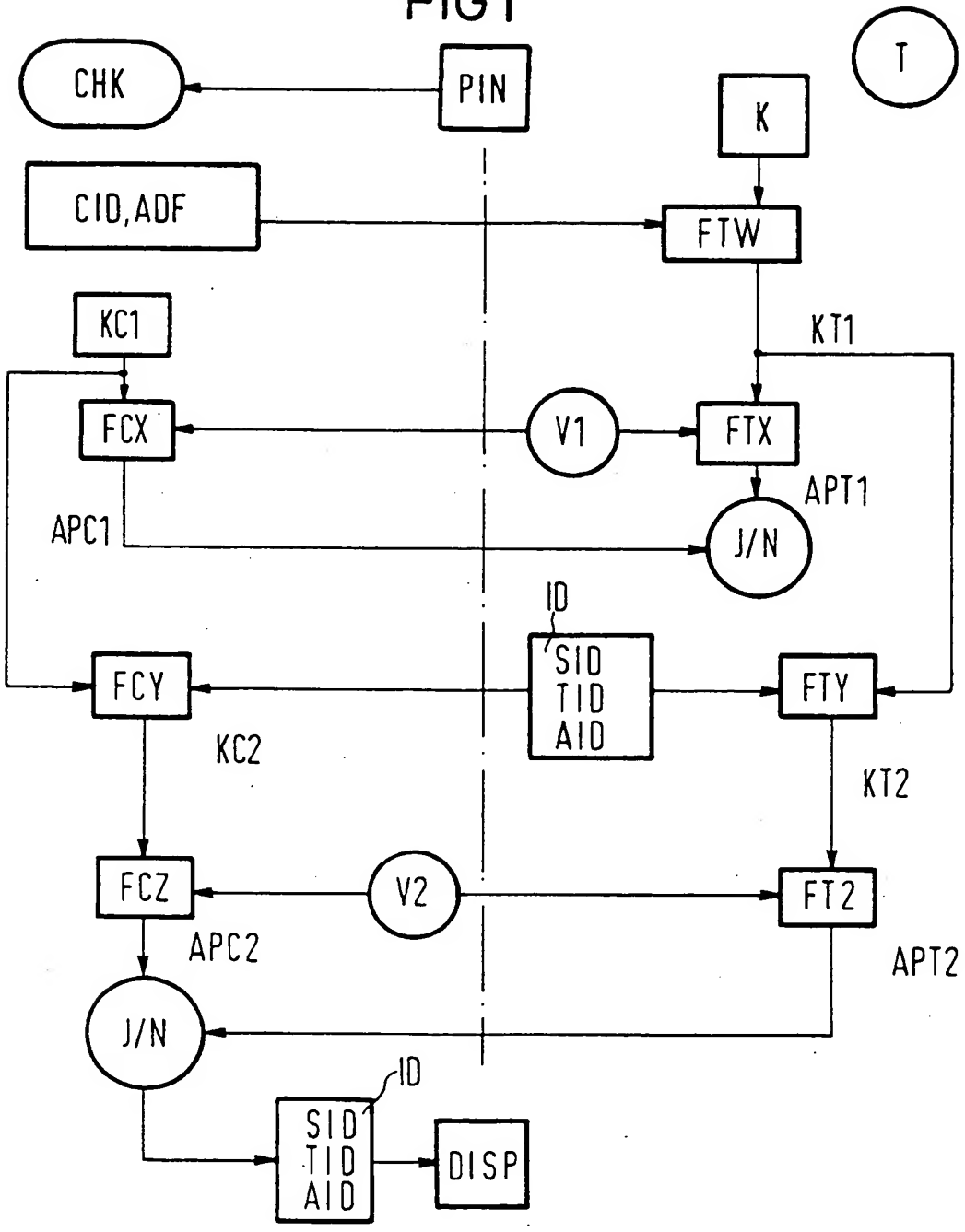

CHK
PIN
T
K
CID,ADF
FTW
KC1
KT1
FCX
V1
FTX
APT1
APC1
J/N
ID
SID
TID
AID
FCY
FTY
KC2
KT2
FCZ
V2
FT2
APC2
APT2
J/N
ID
SID
TID
AID
DISP

FIG 2

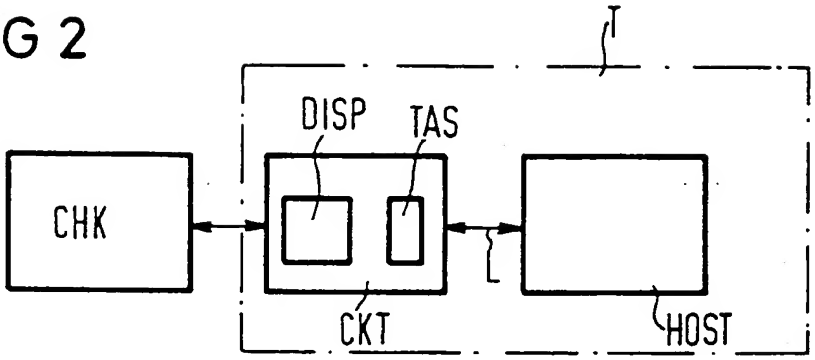
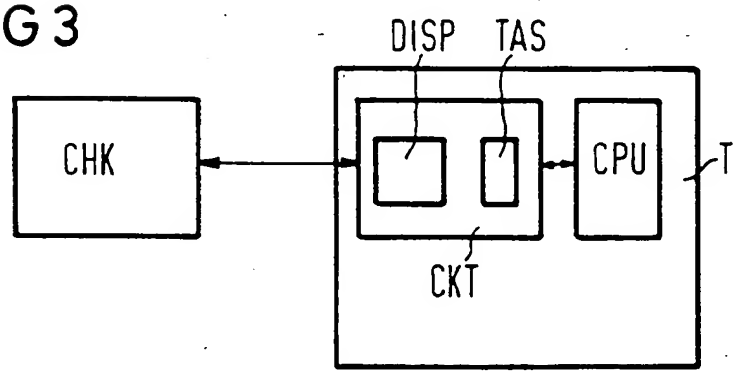


FIG 3



Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 92 10 1016

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.5)
Y	EP-A-0 388 700 (SIEMENS) * Zusammenfassung; Anspruch 1; Abbildungen 1,2 * * Spalte 2, Zeile 24 - Zeile 45 *	1	G07F7/10 H04L9/32
Y	IT INFORMATIONSTECHNIK Bd. 32, Nr. 1, Februar 1990, MÜNCHEN Seiten 64 - 67 , XP000095908 G. KUNDE, D. KRUSE 'Der neue Flughafen München - Sicherheit durch Chipkarten' * Seite 65, Spalte 2, Absatz 3 - Seite 66, Spalte 1, Absatz 1; Abbildungen 1,2 *	1	
A		2,4,10	
A	EP-A-0 400 441 (SIEMENS) * Zusammenfassung; Ansprüche; Abbildung *	1,3	
A	GB-A-2 144 564 (PHILIPS' GLOEILAMPENFABRIEKEN)		
A	GB-A-2 227 111 (TOSHIBA)		

RECHERCHIERTE SACHGEBIETE (Int. Cl.5)
G07F H04L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Rechercheort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	05 OKTOBER 1992	DAVID J.Y.H.

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P0403)

B1

Method for mutual authentification of an IC-card and a terminal.

Veröffentlichungsnummer EP0552392
Veröffentlichungsdatum: 1993-07-28
Erfinder HEWEL HARALD DIPL-ING (DE); KRUSE DIETRICH DIPL-ING (DE); GEFROERER STANISLAUS DIPL-MATH (DE)
Anmelder: SIEMENS NIXDORF INF SYST (DE)
Klassifikation:
- Internationale: G07F7/10; H04L9/32
- Europäische: G07F7/10E; H04L9/32; G07F7/10D4E2
Aktenzeichen: EP19920101016 19920122
Prioritätsaktenzeichen: EP19920101016 19920122

Auch veröffentlicht als
EP0552392 (B1)

Zitierte Dokumente
EP0388700
EP0400441
GB2144564
GB2227111

Zusammenfassung von **EP0552392**

The method specified complements the challenge and response method for mutual authentication of a chip card (CHK) and of a terminal (T). A terminal-specific key (KC2, KT2) is calculated with the aid of identity characteristics (ID) for the terminal (T), the current application and the security module located in the terminal (T), a coding function (FCY, FTY) and the chip-card-specific key (KC1, KT1) prior to authenticity testing of the terminal (T). The identity characteristics (ID) are signalled visually and/or acoustically to the chip-card user after successful conclusion of the authenticity test.

FIG1